

# 將SWA外部身份驗證配置為ISE作為RADIUS伺服器

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路拓撲](#)

[設定](#)

[ISE 組態](#)

[SWA配置](#)

[驗證](#)

[相關資訊](#)

---

## 簡介

本文檔介紹將思科ISE作為RADIUS伺服器在安全Web訪問(SWA)上配置外部身份驗證的步驟。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Secure Web Appliance的基本知識。
- 瞭解ISE上的身份驗證和授權策略配置。
- 基本RADIUS知識。

思科建議您：

- SWA和ISE管理訪問。
- 相容的WSA和ISE版本。

### 採用元件

本檔案中的資訊是根據以下軟體版本：

- SWA 14.0.2-012
- ISE 3.0.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

為SWA的管理使用者啟用外部身份驗證時，裝置會使用外部身份驗證配置中指定的輕型目錄訪問協定(LDAP)或RADIUS伺服器驗證使用者憑證。

## 網路拓撲



網路拓撲圖

管理使用者使用其憑據訪問埠443上的SWA。SWA使用RADIUS伺服器驗證憑證。

## 設定

### ISE 組態

步驟 1. 新增網路裝置。導航到管理>網路資源>網路裝置> +增加。

Network Devices

Name	IP/Mask	Profile Name	Location	Type
No data available				

在ISE中增加SWA作為網路裝置

步驟 2. 為網路裝置對象分配名稱並插入SWA IP地址。

選中RADIUS 覈取方塊並定義共用金鑰。



注意：稍後必須使用相同的金鑰在SWA中配置RADIUS伺服器。

---

Network Devices

Default Device

Device Security Settings

Network Devices List > SWA

Network Devices

\* Name

Description

IP Address  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

**RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

配置SWA網路裝置共用金鑰

步驟 2.1. 按一下Submit。

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol **RADIUS**

\* Shared Secret

Use Second Shared Secret  ⓘ

CoA Port

**RADIUS DTLS Settings ⓘ**

DTLS Required  ⓘ

Shared Secret  ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA  ⓘ

DNS Name

**General Settings**

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

提交網路裝置配置

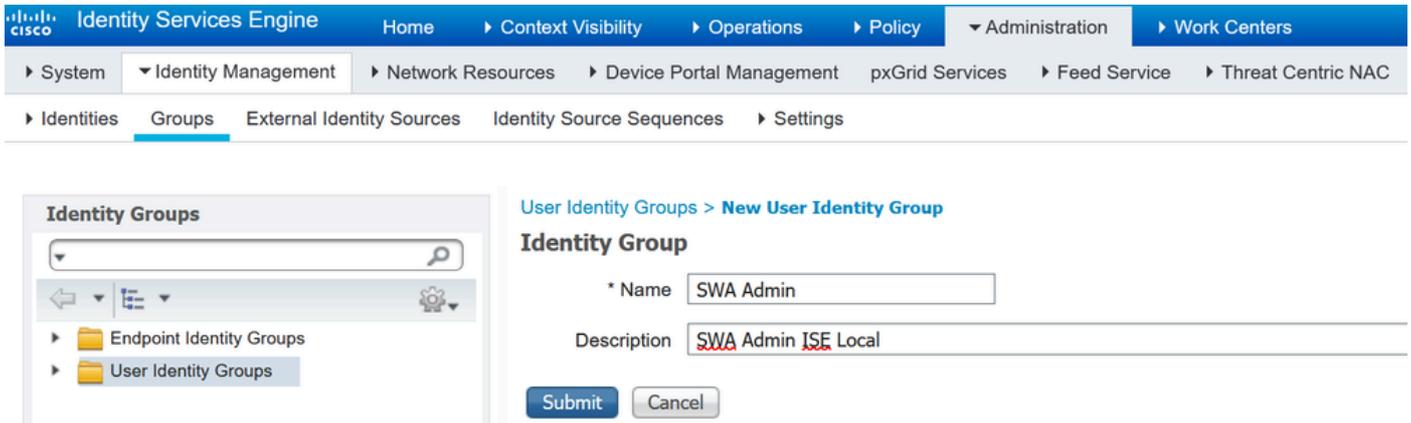
步驟 3. 建立所需的使用者身份組。導航到Administration > Identity Management > Groups > User Identity Groups > + Add。

注意：您需要配置不同的使用者組以匹配不同型別的使用者。

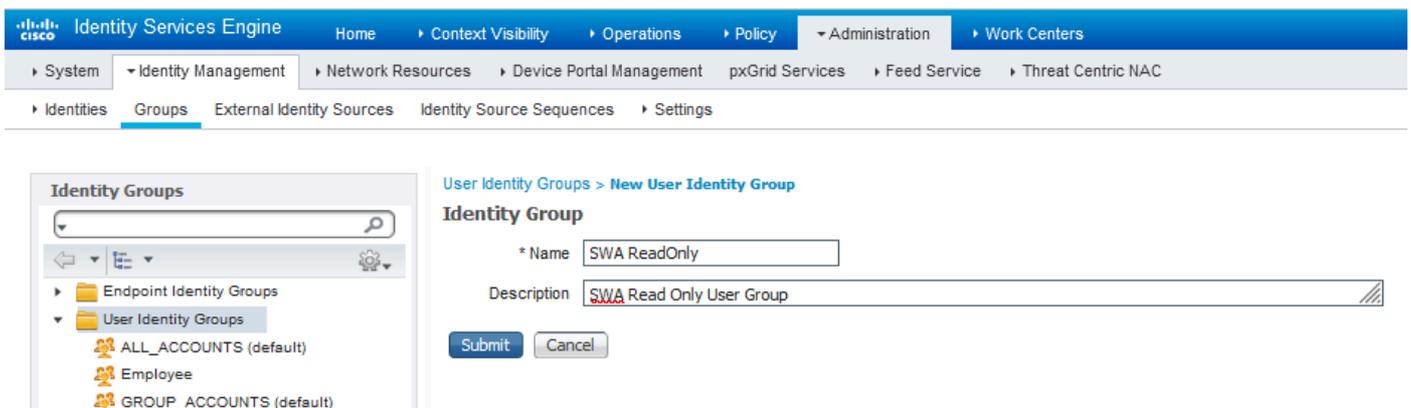
Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type

增加使用者身份組

步驟 4. 輸入組名、說明（可選）和提交。對每個群組重複這些步驟。在本例中，您為管理員使用者建立一個組，為只讀使用者建立一個組。



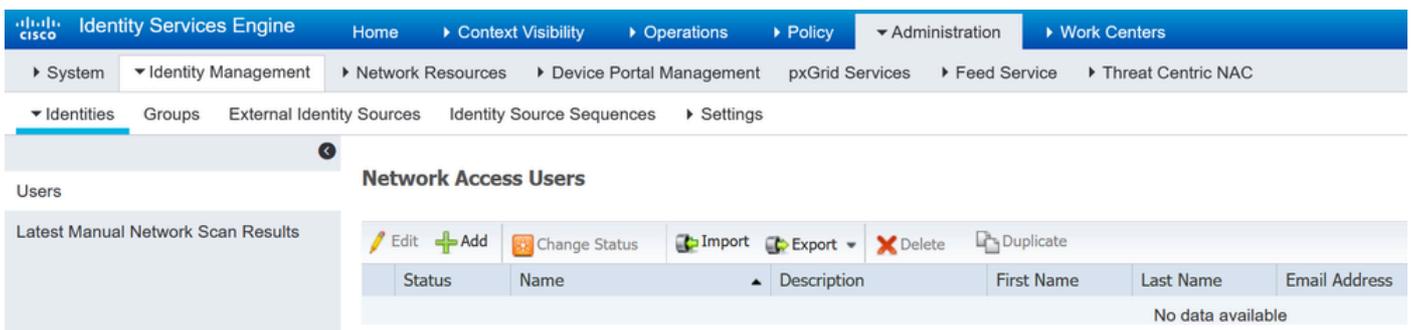
增加使用者身份



組為SWA只讀使用者增加使用者身份組

步驟 5. 您需要建立與SWA中配置的使用者名稱匹配的網路訪問使用者。

建立網路訪問使用者並將他們增加到其對應組。導航到管理>身份管理>身份> + Add。



在ISE中增加本地使用者

步驟 5.1. 您需要建立具有管理員許可權的網路訪問使用者。指定名稱和密碼。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

\* Name

Status  Enabled

Email

Passwords

Password Type:

Password  Re-Enter Password

\* Login Password

增加管理員使用者

步驟 5.2.在User Groups部分中選擇SWA Admin。

Account Disable Policy

Disable account if date exceeds  (yyyy-mm-dd)

User Groups

將Admin Group分配給Admin使用者

步驟 5.3.您需要建立具有唯讀許可權的使用者。指定名稱和密碼。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

\* Name: rouser

Status:  Enabled

Email:

**Passwords**

Password Type: Internal Users

Password: \* Login Password

Re-Enter Password:

Enable Password:

Generate Password (i)

Generate Password (i)

增加只讀使用者

步驟 5.4. 在User Groups部分中選擇SWA ReadOnly。

**Account Disable Policy**

Disable account if date exceeds 2024-03-28 (yyyy-mm-dd)

**User Groups**

SWA ReadOnly

Submit Cancel

將只讀使用者組分配給只讀使用者

步驟 6. 為Admin使用者建立授權配置檔案。

導航到策略>策略元素>結果>授權>授權配置檔案> +增加。

定義授權配置檔案的名稱，並確保訪問型別設定為ACCESS\_ACCEPT。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

\* Name SWA Admin

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

為管理員使用者增加授權配置檔案

步驟 6.1. 在「高級屬性設定」中，導航到 Radius > Class—[25]，輸入值 Administrator，然後按一下 Submit。

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS\_ACCEPT

Class = Administrator

Submit Cancel

為管理員使用者增加授權配置檔案

步驟 7. 重複步驟6為只讀使用者建立授權配置檔案。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

\* Name SWA ReadOnly

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

為只讀使用者增加授權配置檔案

步驟 7.1.這次建立值為ReadUser的Radius : Class , 而非Administrator。

### Advanced Attributes Settings

Radius:Class = ReadUser

### Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = ReadUser

Submit Cancel

為只讀使用者增加授權配置檔案

步驟 8. 建立與SWA IP地址匹配的策略集。這是為了防止使用這些使用者憑證訪問其他裝置。

導航到策略>策略集，點選位於左上角的+圖示。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				

在ISE中增加策略集

步驟 8.1. 新行將放置在策略集的頂部。

為新策略命名，並為RADIUS NAS-IP-Address屬性增加一個條件以匹配SWA IP地址。

按一下Use以保留更改並退出編輯器。

Conditions Studio

Library

Search by Name

- Catalyst\_Switch\_Local\_Web\_Authentication
- Switch\_Local\_Web\_Authentication
- Switch\_Web\_Authentication
- Wired\_802.1X
- Wired\_MAB
- Wireless\_802.1X
- Wireless\_Access
- Wireless\_MAB
- WLC\_Web\_Authentication

Editor

Radius-NAS-IP-Address

Equals 10.106.38.176

Set to 'Is not' Duplicate Save

+ New AND OR

Close Use

增加策略以對映SWA網路裝置

步驟 8.2. 按一下Save。

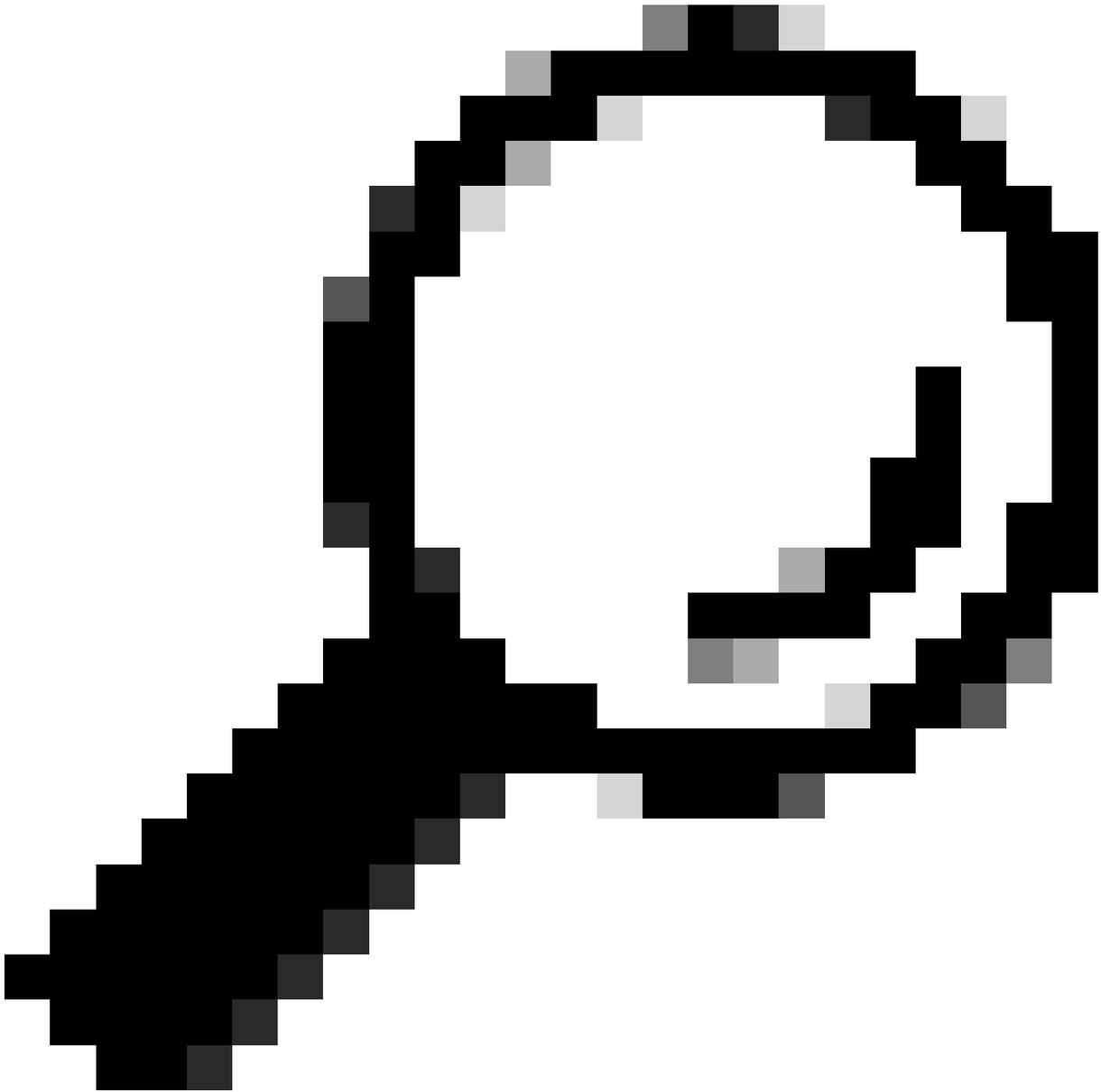
Policy Sets

Reset Policyset Hitcounts Reset Save

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access x +		⚙️	➔
	✓	Default	Default policy set		Default Network Access x +	0	⚙️	➔

Reset Save

策略儲存



提示：在本文中，允許使用預設網路訪問協定清單。您可以建立新清單，並視需要縮小範圍。

---

步驟 9. 要檢視新的策略集，請點選檢視列中的 > 圖示。展開 Authorization Policy 選單，然後按一下 + 圖示以增加新規則，以允許對具有管理員許可權的使用者進行訪問。

設定名稱。

步驟 9.1. 要建立匹配管理員使用者組的條件，請點選 + 圖示。

▼ Authorization Policy (0)

	Status	Rule Name	Conditions
Search			
		SWA Admin	

增加授權策略條件

步驟 9.2. 設定條件以匹配屬性名稱等於使用者身份組的身份組SWA admin。選

### Conditions Studio

#### Library

Search by Name

📍 🗨️ 📄 📁 🌐 🖨️ 📧 📅 🕒 🧑 🗑️ 📶

BYOD_is_Registered	
Catalyst_Switch_Local_Web_Authentication	
Compliance_Unknown_Devices	
Compliant_Devices	
EAP-MSCHAPv2	
EAP-TLS	
Guest_Flow	
MAC_in_SAN	
Network_Access_Authentication_Passed	
Non_Cisco_Profiled_Phones	
Non_Compliant_Devices	
Switch_Local_Web_Authentication	

#### Editor

Click to add an attribute

Select attribute for condition

📍 🗨️ 📄 📁 🌐 🖨️ 📧 📅 🕒 🧑 🗑️ 📶

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
AD	ExternalGroups		
CWA	CWA_ExternalGroups		
IdentityGroup	Description		
<b>IdentityGroup</b>	<b>Name</b>		
InternalUser	IdentityGroup		
PassiveID	PassiveID_Groups		

Close

Use

擇身份組作為條件

步驟 9.3. 向下滾動並選擇User Identity Groups : SWA admin.



步驟 10. 點選+圖示增加第二條規則，以允許訪問具有只讀許可權的使用者。

設定名稱。

設定條件以匹配Dictionary Identity Group和Attribute Name Equals User Identity Groups : SWA ReadOnly，然後按一下Use。

Conditions Studio

Library

Search by Name

BYOD\_is\_Registered

Catalyst\_Switch\_Local\_Web\_Authentication

Compliance\_Unknown\_Devices

Compliant\_Devices

EAP-MSCHAPv2

EAP-TLS

Guest\_Flow

MAC\_in\_SAN

Network\_Access\_Authentication\_Passed

Non\_Cisco\_Profiling\_Phones

Editor

IdentityGroup-Name

Equals

\*User Identity Groups:SWA ReadOnly

Set to 'Is not'

Duplicate

Save

+ New AND OR

Close Use

選擇只讀使用者組的授權策略

步驟 11. 分別為每個規則設定Authorization Profile，然後按一下Save。

Policy Sets → SWA Access

Reset Pollicyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access	0

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

	Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
✎	✓	SWA Read Only	IdentityGroup-Name EQUALS User Identity Groups:SWA ReadOnly	* SWA ReadOnly	Select from list		⚙️
✎	✓	SWA Admin	IdentityGroup-Name EQUALS User Identity Groups:SWA Admin	* SWA Admin	Select from list		⚙️
	✓	Default		* DenyAccess	Select from list	0	⚙️

Reset Save

選擇授權配置檔案

## SWA配置

步驟 1. 從SWA GUI導航至系統管理，然後按一下使用者。

步驟 2. 在External Authentication中按一下Enable。

The screenshot displays the Cisco Secure Web Appliance (S100V) GUI. The navigation bar at the top shows 'System Administration' as the active tab. Below the navigation bar, the 'Users' section is visible, featuring a table with columns for 'All Accounts', 'User Name', 'Full Name', 'User Type', 'Account Status', 'Passphrase Expires', and 'Delete'. A single user entry is shown with 'admin' as the user name and 'Administrator' as the user type. Below the table, there are buttons for 'Add User...' and 'Enforce Passphrase Changes'. The 'Local User Account & Passphrase Settings' section shows 'Account Lock' and 'Passphrase Reset' as 'Not configured', and 'Passphrase Rules' as 'Require at least 8 characters. Additional rules configured...'. The 'External Authentication' section is currently disabled, and a red arrow points to the 'Enable...' button. The 'Second Factor Authentication Settings' section is also disabled, with an 'Enable...' button at the bottom right.

在SWA中啟用外部身份驗證

步驟 3. 在RADIUS伺服器主機名欄位中輸入ISE的IP地址或FQDN，並輸入在步驟2 ISE配置中配置的相同共用金鑰。

步驟 4. 在Group Mapping中選擇Map external authenticated users to multiple local roles。

步驟 4.1. 在「RADIUS CLASS Attribute」欄位中輸入Administrator，然後選擇Role Administrator。

步驟 4.2. 在RADIUS CLASS Attribute欄位中輸入ReadUser並選擇角色只讀運算子。



### Edit External Authentication

**External Authentication Settings**

**Enable External Authentication**

Authentication Mode: Password based Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:							Add Row
RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Certificate		
10.106.38.150	1812	*****	5	PAP	Select any		

External Authentication Cache Timeout: 0 seconds

Group Mapping:

Map externally authenticated users to multiple local roles. (recommended)

RADIUS CLASS Attribute	Role	Add Row
administrator	Administrator	
ReadUser	Read-Only Operator	

*RADIUS CLASS attributes are case-sensitive.*

Map all externally authenticated users to the Administrator role.

Cancel Submit

#### RADIUS伺服器的外部身份驗證配置

第5步：要在SWA中配置使用者，請點選增加使用者。輸入使用者名稱並選擇所需角色所需的使用者型別。輸入Passphrase和Retype Passphrase，如果裝置無法連線到任何外部RADIUS伺服器，則需要此密碼才能進行GUI訪問。

注意：如果裝置無法連線到任何外部伺服器，它會嘗試將使用者驗證為在Secure Web裝置上定義的本地使用者。

## Users

Users						
Add User...						
<small>* When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.</small>						
<input type="checkbox"/> Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	
<input type="checkbox"/>	rouser	RO User	Read-Only Operator	Active	n/a	

SWA中的使用者配置

第6步：點選提交和提交更改。

## 驗證

使用配置的使用者憑證訪問SWA GUI，並檢查ISE中的即時日誌。要檢查ISE中的即時日誌，請導航

到操作>即時日誌：

**Overview**

Event	5200 Authentication succeeded
Username	adminuser
Endpoint Id	
Endpoint Profile	
Authentication Policy	SWA Access >> Default
Authorization Policy	SWA Access >> SWA Admin
Authorization Result	SWA Admin

**Authentication Details**

Source Timestamp	2024-01-28 17:28:31.573
Received Timestamp	2024-01-28 17:28:31.573

**Steps**

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Radius.NAS-IP-Address
- 15041 Evaluating Identity Policy
- 22072 Selected identity source sequence - All\_User\_ID\_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - adminuser
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15016 Selected Authorization Profile - SWA Admin
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

驗證使用者登入ISE

## 相關資訊

- [Cisco Secure Web Appliance AsyncOS 14.0使用手冊](#)
- [ISE 3.0管理指南](#)
- [安全Web裝置的ISE相容性清單](#)
- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。